PRESS RELEASE

2011 年 12 月 27 日

報道関係各位

株式会社セキュアブレイン

セキュアブレイン gred セキュリティレポート Vol.29【2011 年 11 月分統計】

－ 2011 年企業・個人を脅かしたインターネットの脅威 －

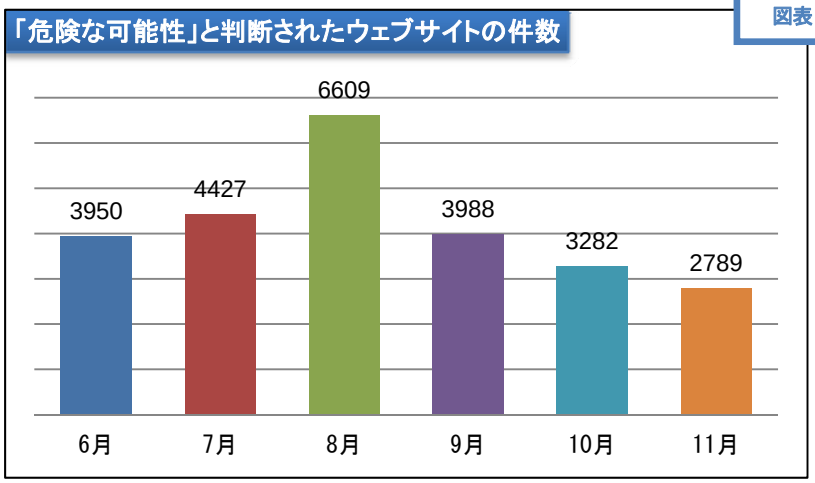
株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)はセキュアブレインが運用する、無料のウェブセキュリティサービス「gred(グレッド)でチェック」で収集した情報を基に、「セキュアブレイン先端技術研究所」(以下 先端技術研究所)で分析を行い、その結果を「セキュアブレイン gred セキュリティレポート」として公表します。「gred でチェック」は、インターネットユーザがウェブサイトの安全確認を行うことができる、無料のウェブセキュリティサービスです。確認したいウェブサイトの URL を入力するだけで、セキュアブレインが独自に開発した解析エンジンが、ブラックリストを使用せず短時間で解析し、そのウェブサイトの安全性を判定します。

内容

1　gred セキュリティレポート概要

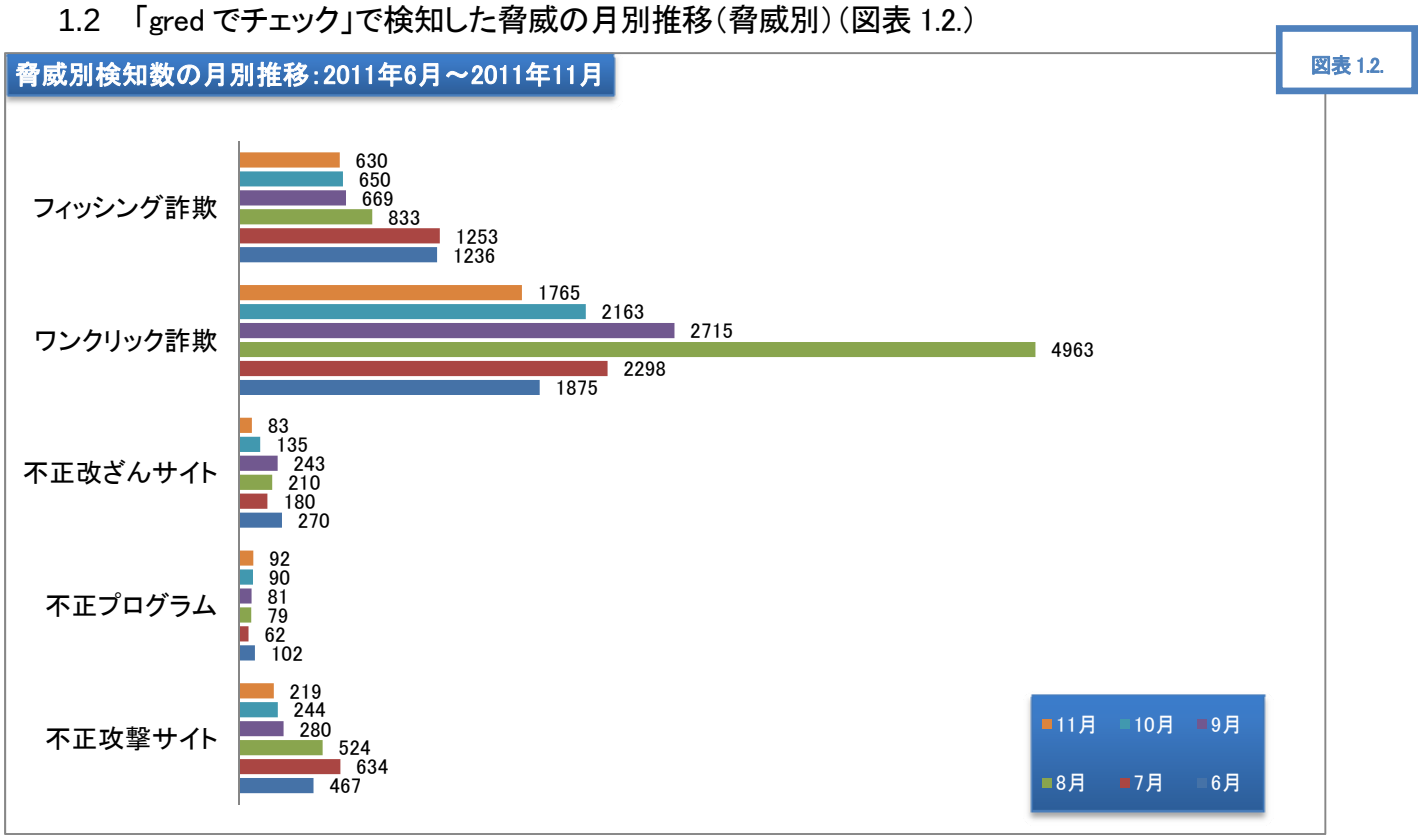
1.1　「危険な可能性のあるウェブサイト」と判断されたウェブサイトの数（図表 1.1.）

図表 1.1



1.2　「gred でチェック」で検知した脅威の月別推移（脅威別）（図表 1.2.）

図表 1.2.



※2011 年 7 月の統計から「ワンクリック不正請求」を「ワンクリック詐欺」としました。

1.3　「gred でチェック」月別総利用数（図表 1.3.）

図表 1.3.

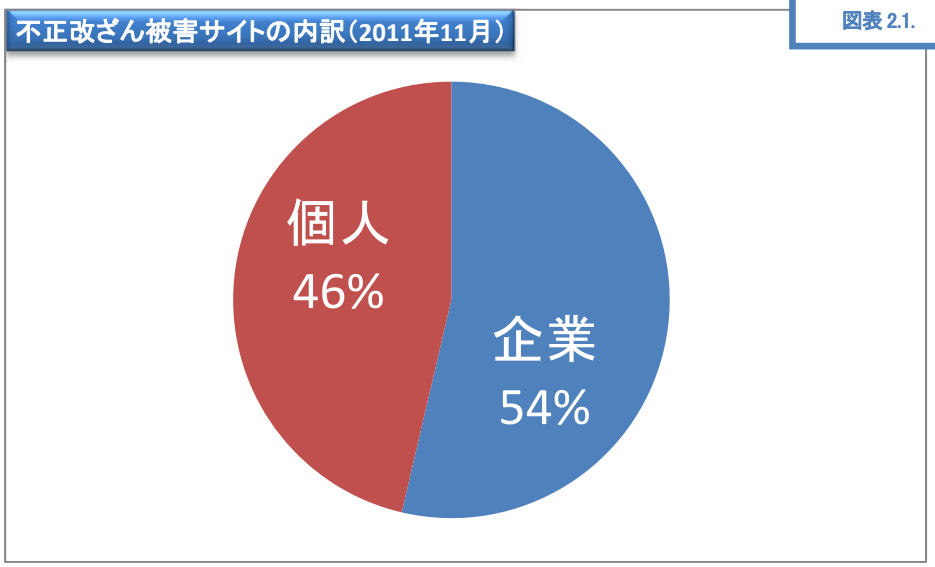
月	6 月	7 月	8 月	9 月	10 月	11 月
「gred でチェック」総利用数	37,915	38,006	44,272	41,269	41,897	39,618

「gred でチェック」のチェック結果に表示される脅威の説明

表示される脅威の名称	説明
フィッシング詐欺	本物そっくりに、偽造されたウェブサイトです。ユーザの ID や、パスワード等の個人情報を不正に取得します。
ワンクリック詐欺	ウェブサイト上のボタン等をクリックしただけで、契約が成立したように見せかけ、料金を不当に請求する詐欺を行っているウェブサイトです。
偽ソフトウェア（不正プログラム）	不当に料金を請求する、実際には機能しない、偽物のソフトウェアを配布しているウェブサイトです。
不正攻撃サイト	他のコンピュータに存在する脆弱性を突いて、攻撃を行うことを目的として作成されたウェブサイトです。
不正改ざんサイト	攻撃者によって、不正に改ざんされてしまった状態になっているウェブサイトです。
ウイルス（不正プログラム）	ウイルスが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
ワーム（不正プログラム）	電子メールやネットワークを利用し自己増殖する、ワームが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
スパイウェア（不正プログラム）	個人情報等をコンピュータから盗む、スパイウェアが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。
その他のマルウェア（不正プログラム）	ウイルス、ワーム、スパイウェア以外の不正プログラムが仕掛けられているウェブサイトです。閲覧すると感染被害の恐れがあります。

2　数値で見る「不正改ざんサイト」の内訳（図表 2.1.、2.2.）

図表 2.1.



図表 2.2.

	2011 年 11 月	2011 年 10 月	2011 年 9 月	2011 年 8 月	2011 年 7 月	2011 年 6 月
「危険な可能性がある」と判断されたウェブサイトに占める「Drive by Download タイプの攻撃」の割合	0.9%（24 件/2,789 件）	1.7%（55 件/3,282 件）	1.9%（77 件/3,988 件）	0.7%（48 件/6,609 件）	2.2%（98 件/4,427 件）	4.2%（166 件/3,950 件）
「不正改ざんサイト」の検知件数に占める「Drive by Download タイプの攻撃」の割合	28.9%（24 件/83 件）	40.7%（55 件/135 件）	31.7%（77 件/243 件）	22.8%（48 件/210 件）	54.4%（98 件/180 件）	61.5%（166 件/270 件）

3　2011 年 企業・個人を脅かしたインターネットの脅威

3.1　2011 年も猛威をふるったウェブサイトの改ざん

狙われる企業ウェブサイト

2010 年から際立った被害が出始めた「企業ウェブサイトの改ざん被害」は、2011 年も猛威をふるいました。特に 2011 年 4 月に「LizaMoon 攻撃」、8 月に「osCommerce の脆弱性を利用した攻撃」等の「Drive by Download タイプの攻撃」により、多くのウェブサイトが被害被っていることを先端技術研究所でも確認しています。

これらの攻撃は、正規ウェブサイトに不正なコードを埋め込み、そのウェブサイトの閲覧者を「マルウェア等の不正プログラムを配布しているウェブサイト」、「フィッシング詐欺サイト」、「ワンクリック詐欺サイト」等のいわゆる「危険なウェブサイト」への誘導を行い、企業の機密情報や個人情報の搾取等の攻撃を行います。

進化・長期化する攻撃

攻撃手法も進化しています。「osCommerce の脆弱性を利用した攻撃」では、ウェブサイト毎に埋め込まれる不正なコードや、誘導される URL が複数存在していることが確認されています。攻撃者はセキュリティソフト等の監視の目から逃れ、できるだけ長い期間に渡って（情報の搾取等の）攻撃を行うために、様々な攻撃手法を使用しています。

既に改ざんが行われたウェブサイトにおいて、再び別の不正コードが埋め込まれる事例も確認されています。不正なコードが埋めこまれても、ウェブコンテンツのソースを確認しない限り、改ざんされたことはわかりません。しかしウェブサイトの管理者が、すべてのコンテンツをリアルタイムに確認することは事実上不可能です。

今後の焦点は「APT 攻撃」対策

APT（Advanced Persistent Threat）攻撃（以下 APT 攻撃）とは？

特定の企業や政府関連組織を標的に対して、金銭搾取等の目的を持って行われる攻撃の総称です。「標的型攻撃」とも言われます。

「APT 攻撃」の概要

Advanced：ターゲットを攻撃するために様々な攻撃方法を持ちます。

Persistent：継続的に攻撃を行います。

Threat：特定の目的を達成するために臨機応変に攻撃方法を変更します。

米 Sourcefire 社の調査によると、2010 年には 3 億個余りのウイルスが発見されましたが、そのうちの約 75%は単一のシステムでしか見つかっていません。※1

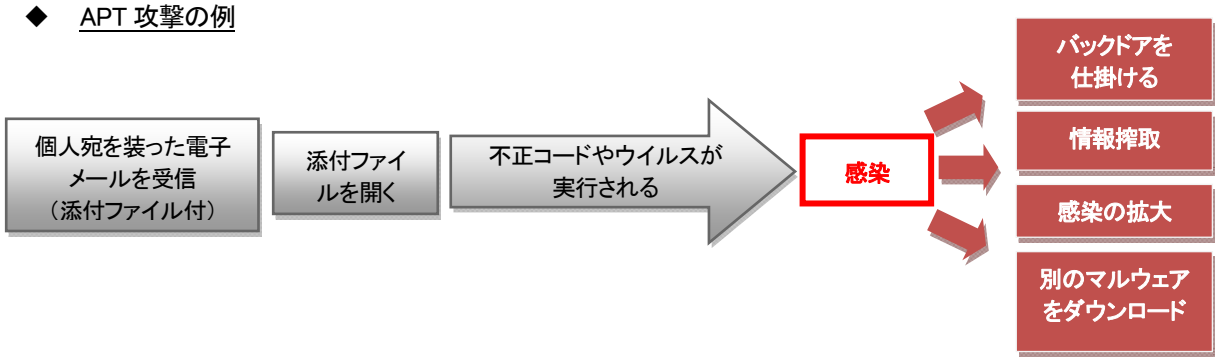
※1：http://www.securityweek.com/agile-security-key-stopping-today%E2%80%99s-high-profile-breaches より引用

つまり、攻撃の多くは不特定多数のシステムやユーザを攻撃対象にするのではなく、ある特定の組織に狙いを定めた「APT 攻撃」であることがわかります。

「APT 攻撃」の例を以下に紹介します。「APT 攻撃」は、「改ざんに使われた不正コードの発見が難しい」、「攻撃に使われるマルウェアがセキュリティソフトで検知できない」等の特徴を持つため、攻撃対象がその被害に気付きにくいという特徴があります。そのため、改ざん被害を受けた多くのウェブサイトでは修正が遅れ、被害が拡大してしまう傾向にあります。

先端技術研究所が確認したところによると、最長 6 ケ月もの間改ざんが放置された例や、一旦は修正したものの、別の攻撃で再び改ざんされたウェブサイトも確認されています。

◆ APT 攻撃の例



3.2 ワンクリック詐欺の攻撃手法が多様化

無料のアダルト動画サイトに貼られる「ワンクリック詐欺サイト」の広告

ワンクリック詐欺サイトの攻撃手法について先端技術研究所で調査を行ったところ、「ワンクリック詐欺サイト」への誘導の窓口として「クリック課金型広告」が活用されている事が分かりました。従来はスパムメールが主な誘導手口でしたが、セキュリティソフトの「スパム対策」の性能向上により、以前ほど詐欺行為の効果が上がらなくなっているため、「ワンクリック詐欺サイト」を運営している犯罪者が、インターネットユーザを誘導する為に「クリック課金型広告」の広告枠を購入していると思われます。

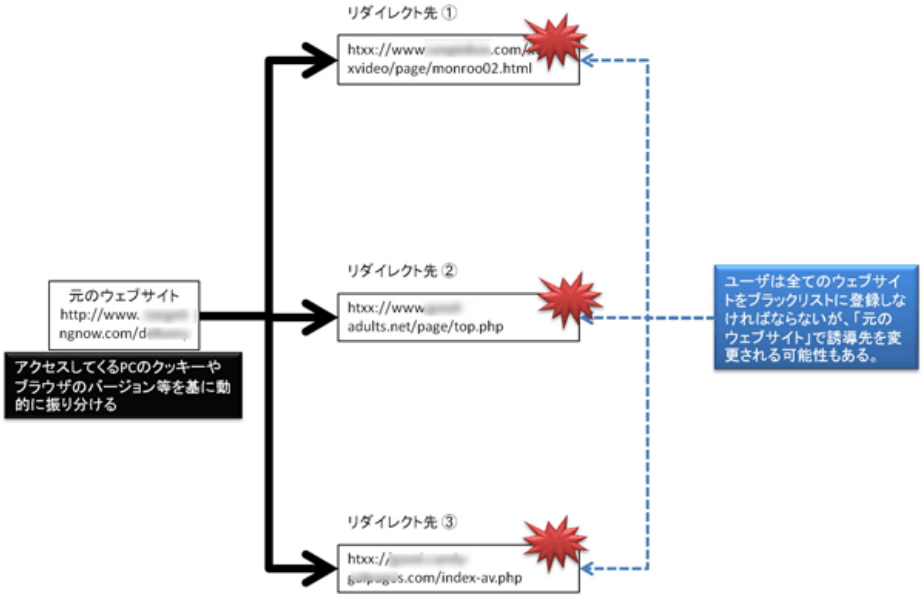
上記画像の右側の部分は、直接「ワンクリック詐欺サイト」へはリンクしていません。画像がリンクしている URL は、「http://[クリック課金型広告を提供する事業者のドメイン]/xxxxx/xxxx.gif」です。

広告枠を管理している会社のドメインを経由して「ワンクリック詐欺サイト」に誘導しています。

「クリック課金型広告」は、広告が「クリック」されることで広告出稿主に課金される仕組みですが、「ワンクリック詐欺サイト」に誘導しても、お金を騙し取ることができないケースも多々あるはずです。その分を差し引いても利益が出るだけの収益をこの広告を経由して得ている。つまり、それだけ多くの被害者がいるということが考えられます。

セキュリティソフトの検知を逃れる「ワンクリック詐欺サイト」

アクセスしているユーザ PC のクッキーやブラウザのバージョン等を基にして、複数の「ワンクリック詐欺サイト」に自動的に振り分ける手法が確認されています。あるウェブサイトでは、アクセスする度に異なるウェブサイトにリダイレクトされます。リダイレクト先の URL は 3～4 種類ほど存在しています。誘導先の多くは「ワンクリック詐欺」を目的としたウェブサイトであることが確認されています。



4　セキュアブレインがご提供するセキュリティソリューション

4.1　個人向けの対策

ブラウザ専用の詐欺対策ソフト「Internet SagiWall（インターネット・サギウォール）

従来のセキュリティ対策ソフトでは検知することのできない「危険なウェブサイトをブロックします。

[ブロックする悪質サイト]

- フィッシング詐欺サイト
- ワンクリック・ツークリック詐欺サイト
- ウイルス等不正プログラム配布サイト
- Gumblar などによって改ざんされたウェブサイト
- 偽ソフトウェア配布サイト

[機能詳細ページ]

http://www.securebrain.co.jp/sagiwall/index.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

※本製品は、BB ソフトサービス株式会社の製品です。

※Android 端末に対応した、「Internet SagiWall for Android」が「ソフトバンクモバイル」および「Android Market」より提供されています。

ソフトバンクモバイルのページ：http://mb.softbank.jp/mb/service/sagiwall/

Android Market のページ：https://market.android.com/details?id=jp.co.bbss.android.security.sagiwall_softbank

閲覧しようとしているウェブサイトの安全性を無料でチェック

セキュアブレインでは、閲覧しようとしているウェブサイトの安全性を、ブラックリストを使わずに判断する、セキュリティサービス「gred でチェック」（http://www.gred.jp）を無料で提供しています。

安い、軽い、安全、最新型ウイルス対策ソフト「gred アンチウイルス アクセラレータ Plus」

米国の研究機関による、ウイルス検知テストで『100%』の実力

全世界で 200 万人が使用！

軽さと高い安全性を実現した最新型ウイルス対策です。

[gred アンチウイルス アクセラレータ Plus の機能]

- 圧縮ファイルのスキャン
- パッカーにより難読化されたファイルのスキャン
- CD、DVD、USB メモリ経由の脅威をブロック
- 電子メールスキャン
- ルートキットの検知と削除
- レジストリとファイルシステムの修復

[機能詳細ページ]

http://www.gredavx.jp/plus/index.html

【ご購入はこちら】セキュアブレインショップ

http://www.securebrain.co.jp/shop/index.html

4.2 企業向けの対策

月々9,000 円からご利用いただけるウェブサイト監視サービス「gred セキュリティサービス」

企業のウェブサイトの管理者は、自社のウェブサイトの安全性を、自動で定期的に監視するソリューションが必要です。セキュアブレインでは、企業のウェブサイトが不正に改ざんされていないかを定期的に監視し、問題が発見された場合には、即座に管理者に通知する、SaaS 型セキュリティサービス「gred セキュリティサービス」をご提供しています。

■「gred セキュリティサービス」無償トライアルお申込み URL

http://www.securebrain.co.jp/products/gred/trial.html

■「gred セキュリティサービス」の機能詳細説明 URL

http://www.securebrain.co.jp/products/gred/function.html

以上

セキュアブレインについて:

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する日本発のセキュリティの専門企業です。詳細は、www.securebrain.co.jp をご覧ください。

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン 広報担当:丸山 芳生(まるやま よしお)

e-mail:info@securebrain.co.jp

電話:03-3234-3001、FAX:03-3234-3002 〒102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F